

REMARKS

Applicants respectfully traverse and request reconsideration.

Applicants have canceled claims 5, 12, 35 and 44 without prejudice.

Applicants wish to thank the Examiner for the notice that claims 6-9, 13-17 and 45-47 would be allowable if rewritten in independent form. Applicants have amended claims 6, 13 and 45 to include limitations from their corresponding independent claims, as such these claims are in condition for allowance along with corresponding dependent claims which are also believed to add additional novel and non-obvious subject matter. New claim 48 is allowable claim 8 rewritten in independent form.

Claims 1-5, 10, 12, 18, 19, 23, 24, 27, 32, 33, 35-37 and 40-44 stand rejected under 35 U.S.C. §102(b) as being anticipated by Appelbaum. Independent claims 1, 10, 32 and 40 have been amended to include dependent claims as such the pending claims are the same as previously presented. In the "Response to Arguments" section of the final action, it appears that the office action may be misinterpreting the teachings of Appelbaum as compared to the claim language of Applicants' claimed invention. For example, paragraph 5 of the "Response to Arguments" section states that Appelbaum discloses a triple encrypted key and that Ki is a key that is described and "there are different FK keys described for different computers (column 2, lines 40-50)." However, Applicants respectfully note that the triple encrypted key of Appelbaum is distinctly different from Applicants claimed double key package. For example, Appelbaum does not appear to state that the FK keys described are for different computers but to the contrary, specifically states that the FK keys are "a single fixed FK key for all of the computers". As such, Appelbaum merely teaches encrypting Ki with a common symmetric key that is the same for all computers and encrypting that again with Ki and then encrypting that again with the same FK key that is the same for all computers as indicated, for example, in column 2, line 46. As such,

only two keys are used and only symmetric key encryption appears to be described in the Appelbaum reference and not asymmetric encryption as alleged and moreover, only a single symmetric common encryption key FK is used to encrypt key Ki and the key Ki itself is used to encrypt itself.

In contrast, as noted for example in Applicants' Fig. 2, the double key package claimed uses at least three different cryptographic keys to form the double key package. For example, as to independent claims 1, 10, 32, and 40, these claims require the use of a first cryptographic key (Ks1) by a first party, a second encryption key associated with the second party and a third encryption key associated with the third party. The Appelbaum reference does not teach using different encryption keys associated with different parties to encrypt a cryptographic key Ks1 as claimed. Accordingly, these claims are in condition for allowance.

Also as to claim 3, for example, this claim requires among other things, that the double key package includes the decryption key that is used to decrypt the encrypted data protected through a double application of asymmetric public key encryption. As noted above, Appelbaum appears to describe only a symmetric key process and that is why the common FK is used for all computers. The Appelbaum claims (see for example col. 6) and the specification describe that the encryption procedure E uses key Ki and the encryption procedure using the FK key "is the same encryption procedure E using a single fixed key FK for all said computers". As such, the same encryption procedure is used and a same key is used meaning that the encryption process is a symmetric key process. Accordingly, this claim is also believed to be in condition for allowance.

As to claim 4, this claim is also believed to be in condition for allowance based on the above remarks.

As to independent claims 18 and 27, Applicants respectfully reassert the relevant remarks made above with respect to claim 3, again noting that the Appelbaum reference does not describe a double application of asymmetric public key encryption, but to the contrary, appears to merely teach symmetric key encryption. Accordingly, these claims are also in condition for allowance. Their corresponding dependent claims are also in condition for allowance for the same reasons and because they add additional novel and non-obvious subject matter. For example, claim 19 requires the use of a third encryption key and as noted above such an operation is not taught or suggested by the disclosed reference. The other dependent claims add additional novel and non-obvious subject matter.

As to claim 23, Applicants respectfully reassert the relevant remarks made in their last response.

Claims 11, 25, 26 and 31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Appelbaum in view of Perlman. Applicants respectfully reassert the relevant remarks made above and as such these claims are also in condition for allowance.

Claims 20-22, 28-30, 38 and 39 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Appelbaum in view of Wertheimer. These claims are allowable at least by depending on an allowable base claim and also since they add additional novel and non-obvious subject matter. In addition, Applicants respectfully note that even combining the Wertheimer reference with that of Appelbaum would not result in Applicants' claimed invention as noted above. Moreover, there is no teaching in Appelbaum of a third party based encrypted security token nor the double key package being communicated as required. In addition, using Wertheimer and combining select teachings with Appelbaum would likely result in simply having the signed triple encrypted key of Appelbaum sent to the computer. There is no teaching

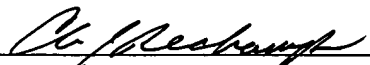
or suggestion of producing a signed message with a third party based encrypted security token.

As such, these claims are also in condition for allowance.

Accordingly, Applicants respectfully submit that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 4/5/04

By: 
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P.C.
222 N. LaSalle Street
Chicago, IL 60601
Telephone: (312) 609-7599
Facsimile: (312) 609-5005
Email: creckamp@vedderprice.com